ADAPTER HAVING SECURE FUNCTION AND COMPUTER SECURE SYSTEM USING IT

Technical Field

This invention relates to adapter ("secure adapter"), to be installed and used between a computer system and a keyboard, which provides security function, and secure computer system using thereof, in particular, to configuration for transferring input information from keyboard to computer system in secure mode by encrypting the data, and for transferring information to computer system in clear mode without encryption.

Background Art

Development of computers and rapid growth of information exchange and communications over Internet has opened the way for quick and easy access to information. In particular, Internet brings a representative paradigm of creating informational environment for individuals, business and e-trade. Internet features openness and conformity, and surmounts difficulties in exchanging and sharing information resources whether used by an individual or a company, whereas the basic drawback of the Internet with respect to information protection and communication safety has been putting serious obstacles. Thus, what is needed is information secure system, which is operable for each service type or application whether communication

is trusted or not, as is the case with information exchange over the Internet, .

While development of information and computer communication enabled electronic transactions such as stock exchange, Internet banking, and other cyber transactions, when using Internet or modem communications, user's information (data) is often drained to other persons by illegal methods including hacking by third persons. For an experienced hacker, information stored on a computer connected to the Internet can be almost as available as the data on the same system. Thus, one cannot say information is safe just because it is stored on someone's computer. Additionally, as technical, marketing and other information is much transferred over the Internet and other media, and electronic transactions and economic activities are frequently performed, it is urgently required to safely protect each individual's information.

Normally, all data inputted from the computer keyboard is transferred, stored and processed in the computer system as is. That it is, the computer operates by using direct connection between the keyboard and the system: the keyboard controller of the computer system receives a key code from the keyboard access port, transmits it to the computer system, and then application program in the computer system receives and uses this value.

Accordingly, if a third person can receive this value from the keyboard port using hacking technique or get it somehow from keyboard controller, this can bring far-reaching effect when an unauthorized person is able to use someone's private data illegally.

Thus, the object of the present invention is to solve the above problems in full and to tackle related technical issues.

That is, the object of the present invention is to prevent information (data) from being drained by other persons using methods not intended by user, such as hacking, enabling the user setting up a secure connection between the computer system and the keyboard for entering data from the keyboard into the computer system .

Also, in the case of with additional safe memory, since the data can be encrypted/decoded only when the user supplies password, and the encryption password is not stored or preserved separately, the present invention can cope with such problems as reproduction and can deal with storing and processing of the data which requires secure handling.

Summary of Invention

To achieve the aforementioned objects, the present invention, which is an adapter to transfer key code input information from the keyboard to the computer system, is configured to transfer the key code input information from the keyboard to the computer system after encrypting it only when the secure mode setup command is received from the keyboard or the computer system, and to transfer the information from the keyboard to the computer system without encrypting the data if the secure mode clear command is received or when in the clear secure mode state.

At the secure mode, the encrypted key code input information may be the

information from all key codes, and only the character and numeral key codes other than special key codes, depending on setup configuration.

Secure mode can be setup/cleared by using a special key ("secure key"), which is additionally installed on the keyboard, or using a combination of existing keys (e.g., CTRL key + ALT key + SHIFT key + S key). Also, the application program under execution in the computer system can set up or clear the secure mode depending on the given conditions, although the user does not control the secure mode with the key.

Disclosure of Invention

The configuration, for example, of a secure adapter for secure mode setup/clearing comprises the main processor to process secure mode setup/clearing commands and to create the secrete key in secure mode setting, the initial cipher to transfer the secrete key transmitted from the main processor to the keyboard controller of the computer system by encrypting the secrete key with the secure key from the computer system, and the stream cipher to encrypt the key code input information from the keyboard with the secrete key.

With reference to Fig. 1, more detailed configuration, as possible embodiment of the secure adapter in the present invention, comprises:

a computer connection coupled to the keyboard port of the computer;

a keyboard connection coupled to the keyboard plug;

a transmit/receive control on the computer to control communication with the computer system;

a transmit/receive control on the keyboard to control communication with the keyboard;

a main processor to create a secrete key, to perform secure mode setup/clearing according to the secure mode commands, and to exchange the data between the computer system and the keyboard;

an initial cipher to encrypt the secrete key transferred from the main processor with the secure key from the computer system and then transmit the encrypted secret key to the computer system when the secure mode is set up; and,

a stream cipher to encrypt the key code input information with the secrete key from the main processor and then to transmit the encrypted information to the computer system when the secure mode is set up.

Said transmit/receive control on the computer writes all information to be transmitted on the input buffer first so that the control program transmits it at a proper time, and all received messages are written on the input buffer and can be used in other modules.

Said transmit/receive control on the keyboard transmits the key code input information from the keyboard to the main processor, all commands transmitted are written on the buffer and this module transmits them at a proper time.

Said stream cipher encrypts information transmitted from the main processor with the secrete key. While each different encryption function is applied because bits or characters of a plain text are encrypted, and thus different encryption function is applied and respective plain text bit is encrypted irregardless of other bits for stream cipher,

unlike block cipher for which the same encryption function is applied to all plain texts, its encrypting speed is relatively high. Also, the impact of channel errors occurring in a certain bit during encryption or transmission process is advantageously applied only to the corresponding bit, but not propagated to other bits. However, configuration using block cipher instead of stream password can be used, if necessary.

For computer connection and keyboard connection, 5V power is normally supplied, and they are connected with a communication line. However, the secure adapter of the present invention is not necessarily to be a device separated from the keyboard and the computer system in design, and can be coupled with the computer body or with the keyboard. In this case, the transmit/receive means of the computer body and the keyboard may not be a cable, but the system can be designed so that radio information transmitter is installed on the keyboard and radio information receiver is installed on the computer body. In the Fig. 2, an example of a secure adapter connected between the computer system and the keyboard as an independent device is shown. On the secure adapter, an indication lamp showing operating state and a secure mode indication lamp (described below) are installed.

A secure adapter of the present invention may include one or more indication lamps. These indication lamps show the operation mode of the secure adapter, the secure mode indication lamp shows secure state, and so on. In this case, the secure mode indication lamp is controlled by the main processor. Under secure mode, the secure mode indication lamp is on, and goes off when secure mode is cleared, while the lamp periodically blinks when secure mode state is disabled. The disabled secure mode state means the case when setting of the computer system, the secure key and/or the

secrete key was not performed normally. The secure mode indication lamp is not only installed on the secure adapter, but on the front of the computer body, the keyboard or on the monitor as the case may be. If necessary, a small indicator (i.e., an icon type, etc.) can be displayed on the setup screen on the monitor to prompt whether the secure mode is set up or not.

Depending on the case, safe memory interworking with the main configuration of the secure adapter may be added. Said safe memory operates under the secure mode that an application program executed on the computer system established in necessary case, and is used for storing and processing encrypted data which requires separate security handling.

More specifically, said safe memory comprises:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and

calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface.

In this case, the main processor of the secure adapter additionally has a function to transmit the password input request command to the computer system where the secure mode setup command received from the application program of the computer system is for the safe memory, and to transmit the password received from the keyboard to the safe memory.

The safe memory does not store password separately, and executes decoding using the safe key converted from the password only when the user enters the same

password as the password used for storing the encrypted data. Whether the correct password is entered is acknowledged as valid access only when values are the same after comparing the "password integrity identification value" stored in the encrypted data of the data storage memory with the "password integrity identification value" calculated after encryption with the safe key converted from the newly entered password.

Therefore, the safe key transferred from the encryption/key operation processor to the decoder is temporally stored on the buffer of the decoder and then the key is deleted from the buffer by the command from the comparison/processor, where the stored "password integrity identification value" and the "password integrity identification value" calculated from the newly entered password are not the same, as the result of execution of the comparison/processor.

The conversion of password to a safe key may be executed using various known methods such as hash function or polynomial algorithms. Representative examples are the MAC hash function, the MDC hash function, the MD4 hash function, the MD5 hash function, the SHA hash function, the CRC algorithm, and so on.

The integrity identification protects data against hacker's active attacks because it is used as a means to identify the person who performs the access. As a method to identify the integrity, various known algorithms described above can be used, in particular Cyclic Redundancy Checking (CRC) algorithm is preferred. In transmitting the data of K bits, the CRC algorithm transmits the data of k+n bits by dividing the transmitted data into n+1 bit patterns and adding the remaining of n bits length occurred

at the division to the end of data bits. The algorithm can be adjusted so that the data is organized as n bits at the point to receive the data and the received data is divided by the pattern, and then data transmission errors are found through the remaining values. Where the remainder is 0 at the point to receive the data, it is considered that there are no data transmission errors, and there are data transmission errors where it is 1. Accordingly, in the present invention, the data transmission error identification algorithm configuration in communication is transformed and used, as the method to store the values to the data storage memory by calculating the CRC value ("encrypted data CRC value") of the data encrypted with the safe key converted from password and the CRC value of password ("password CRC value"), and to compare the "password CRC value" calculated from the password entered by the user with the "password CRC value" stored on the data storage memory when an application program of the computer system intends to acquire the data under the secure state. Thus, if the stored CRC value and the newly calculated CRC value are the same, it is confirmed that the user who entered the same password with the password used in data storage has now access to the computer system. In the above, n is 16 or 32 bits. In the present invention, 16 bits are preferably used.

The encryption algorithm used for encrypting with the safe key can be selected among various known encryption algorithms, or a separate algorithm can be developed and used.

The "password integrity identification value" and the "encrypted data integrity identification value" are stored together in the data storage memory, the "password integrity identification value" being used to identify whether the password to newly

enter data is correct, while the "encrypted data integrity identification value" being used to identify whether the encrypted data is stored without errors or with errors during storage. That is, it is possible to identify the above by repeatedly encrypting the decoded data with the safe key, calculating the integrity identification value of the encrypted data, and comparing the value with the encrypted data integrity identification value written on the data storage memory. Therefore, it is possible to confirm whether errors occurred in storing or decoding the encrypted data, by adding a separate module that can execute such a function or adding such a function to the basic configuration module.

On the other hand, if each different password is used in storing the multitude of encrypted data at the same time or several times to the data storage memory, a different "password integrity identification value" is stored respectively for the encrypted data. That is to say, passwords may be set differently in storing data, and thus may be specific to the type of encrypted data. Accordingly, if necessary, it is possible to establish the password integrity identification value of the encrypted data stored on the data storage memory depending on the type of encrypted data. In the drain process of the encrypted data, all encrypted data with the same "password integrity identification value" are decoded.

The encryption algorithm used in the safe memory may differ from the encryption algorithm used in the stream cipher of the secure adapter.

The present invention also relates to the computer security system, which comprises the secure adapter, the keyboard and the computer system.

A separate secure key for entering the secure mode setup/clearing command is incorporated in the keyboard and/or the secure mode setup/clearing command is created by the combination of existing key codes. The computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and includes the keyboard manager with application program interface. The application program interface has the function to perform direct decoding in the application program of the computer system and/or provides the function with which the operating system of the computer system can perform decoding.

The secure key created in the keyboard manager of the computer system is transmitted to the secure adapter in setting the secure mode. When the secure key transmitted to the secure adapter encrypts the newly created secrete key from the adapter in each secure mode setup, and then retransmits the encrypted secrete key to the computer system. The secure adapter transmits the key code value entered from the keyboard to the computer system after encrypting the value with the secrete key. Then, the computer system processes the encrypted key code input information transmitted from the secure adapter after decoding the information with the stored secrete key.

The computer system includes general operating system, application programs and so on in addition to the keyboard manager. The function to decode encrypted information may be incorporated to the keyboard manager, the operating system and/or application programs. Wherein, there are protocols between application programs and the keyboard manager, and between the operating system and the keyboard manager, to acquire the decoded information. This is to prevent the case that a third person can

misuse the external interface of the keyboard for hacking purposes.

Referring now to the Fig.3, an example that the computer system can be executed under Microsoft Windows 98 and the keyboard manager has the decoding function is described below. However, in addition to Windows 98, corresponding protocols are applicable for Windows 2000, Windows/NT, Unix, Linux and so on.

When the computer system is operated, the keyboard manager makes and sends the secure key to the secure adapter. Then the manager receives the secrete key encrypted by the secure key from the secure adapter in secure mode, and then receives key code input information encrypted by the secrete key from the secure adapter. The encrypted key code input information received from the secure adapter by the keyboard manager is not immediately decoded, but stored in a location of the keyboard manager or the computer system and only the signal that any key code is pressed is sent to the application program interface by the operating system.

On the one hand, when an application program needs to examine the transferred key code during operation, the application program interface interrupts the code and requests decoding of the key code first pressed to the keyboard manager. Then the keyboard manager transfers the stored encrypted key code input information to the application program interface after decoding it with the stored secrete key, and then the application program interface returns the decoded information to the application program as the result of examination.

With reference, if booting process of the computing system of the present

invention is checked, BIOS operation, LOADER operation, KERNEL operation, keyboard manager operation and O.S operation is performed in sequence in applying power. Therefore, since the keyboard manager is executed while O.S is being loaded after a computer is energized, the keyboard manager is executed earlier than general hacking or application programs.

On the other hand, when the secure mode is cleared, the keyboard input information is not encrypted and transferred to the keyboard manager and then directly to application programs through the operating system.

Referring now to the Fig.4, an example when safe memory is added to the main configuration of the secure adapter of the present invention is described below. This embodiment is defined to only the case when the integrity identification value is calculated using the CRC algorithm.

If storage or processing commands of the data which requires security together with the secure mode setup command from the application program of the computer system are sent to the main processor, the main processor switches the system to secure mode and sends the password input request command to the computer system. If the computer system prompts for password input on screen, the user supplies the password, the password is transferred to the main processor through the keyboard transmit/receive control, and the main processor sends it to the interface of the safe memory.

If the secure mode setup command from the application program is for data storage requiring security, the data from an application program is transferred to the

main processor and then the main processor receives and transfers the data to the safe memory interface. If the safe memory interface transfers password and the secure data to the encryption/key operation processor, the encryption/key operation processor converts the password to the safe key and encrypts the secure data and the password, using the safe key. On the other hand, the encryption/key operation processor calculates the CRC values of the encrypted password and the encrypted data, and then transmits the "encrypted data", the "password CRC value" and the "encrypted data CRC value" to the comparison/processor. The comparison/processor records the information to the data storage memory (refer to the Fig.8).

In the meantime, if the secure mode setup command from the application program is for decoding the stored encrypted information, only the password transferred to the safe memory interface is sent to the encryption/key operation processor. The encryption/key operation processor encrypts password with the safe key after converting the password to the safe key, calculates the CRC value of the encrypted password ("password CRC value"), and then respectively transmits the "safe key" to the decoder, and the "password CRC value" to the comparison/processor. The comparison/processor scans the data storage memory and confirms whether the "password CRC value" stored in the memory is equal to the "password CRC value" received from the encryption/key operation processor. If two CRC values are equal, the comparison/processor receives and transfers the encrypted data from the data storage memory to the decoder. The decoder decodes the encrypted data from the comparison/processor with the safe key, and deletes the safe key after transmission of the data to the safe memory interface. If two values are not equal, the comparison/processor deletes the safe key stored on the decoder buffer and transmits

password nonconformity to the computer system (refer to Fig.9).

The process that the decoded data is encrypted again with the secrete key in the stream cipher and transmitted to the computer system is the same as the aforementioned description for the main configuration of a secure adapter. However, as the case may be, it is possible to organize the process where the data decoded in and transmitted from the safe memory can be transferred to the computer system without repeated encryption in the stream cipher.

The present invention also relates to a method to secure the key code input information transferred from the keyboard using the secure computer system.

In particular, the method comprises the steps for:

transferring a secure key created in the keyboard manager of the computer system to the secure adapter in computer booting;

creating a new secrete key in the main processor when the secure mode setup command from the keyboard or the computer system is transferred to the main processor of the secure adapter, and then transferring the secrete key to the initial cipher and the stream cipher of the secure adapter;

encrypting the secrete key with the secure key in the initial cipher and then transferring the encrypted secrete key to the keyboard manager through the computer connection by the transmit/receive control on the computer;

under secure mode, main processor transferring the information to the stream cipher if the key code input information of the keyboard is transferred to the main processor through the transmit/receive control on the keyboard, the stream cipher's

encrypting the key code input information with the secrete key and transferring the encrypted information to the keyboard manager through computer connection by the transmit/receive control on the computer;

computer system decoding the encrypted information using the secrete key;

main processor transferring the secure mode clearing command to the stream cipher when the secure mode clearing command is transferred from the keyboard or the computer system to the main processor of the secure adapter; and

when secure mode is cleared, the stream cipher transferring the transferred key code input information to the keyboard manager through the computer connection by the transmit/receive control on the computer without encryption, if the key code input information of the keyboard is transferred to the stream cipher through the transmit/receive control on the keyboard after passing through the keyboard connection.

Where the safe memory is incorporated into the main configuration of a secure adapter, the configuration further comprises the step of: main processor transferring the password from the transmit/receive control on the keyboard and the secure data from the transmit/receive control on the computer to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory encrypting and then storing the received data using the password, if secure mode setup is made by the command from the application program of the computer system and also for data storage requiring security; but

main processor transferring the password from the transmit/receive control on the keyboard to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory decoding the encrypted data with the password and then transferring the decoded data to the main processor

where the password is correct, but not decoding the encrypted data where not correct, if secure mode setup is made by the command from the application program of the computer system and also for acquisition of the secure data.

On the basis of the Fig. 1 operation process of a secure adapter is described below in secure mode setting/clearing by the computer secure system of the present invention.

When the computer is booted (the process when the power is applied, operating system is initiated and then the computer goes into operation state), the keyboard manager of the computer system (not shown) transfers the secure key to the main processor through the computer connection by the transmit/receive control on the computer. The main processor turns on the operating indication lamp and sends the secure key to the initial cipher.

On the other hand, the key code input information from the keyboard is transferred to the main processor through the keyboard connection by the transmit/receive control on the keyboard. The main processor turns on the secure mode indication lamp, creates and transfers the secrete key to the initial cipher and the stream cipher, and also the key code input information to the stream cipher, if the input information transferred from the keyboard is for secure mode setup. The initial cipher encrypts the secrete key with the secure key, and sends the encrypted secrete key to the keyboard manager of the computer system through the computer connection by the transmit/receive control on the computer. On the other hand, the stream cipher transfers the encrypted information to the keyboard manager of the computer system through the

computer connection by the transmit/receive control of the computer after encrypting the key code input information, using the secrete key transmitted from the main processor. The process to handle the encrypted key code input information, transferred to the keyboard manager, in the computer system is referred to the details described before on the Fig.3 basis.

If the secure mode clearing command is directed from the computer system or the keyboard, the clear command is transferred to the main processor and the stream cipher by the transmit/receive control on the computer or the transmit/receive control on the keyboard. The main processor turns off the secure mode indication lamp and transfers the secure mode clearing command to the stream cipher. Thereafter, key code values transferred from the keyboard are transferred to the computer system through the computer connection by the transmit/receive control on the computer, without encryption in the stream cipher.

The process to handle the not-encrypted key code input information, transferred to the keyboard manager in the computer system is referred to the details described before on the basis of the Fig.3.

If the secure key is not acquired from the keyboard manager of the computer system during booting the computer, the secure adapter goes in the disabled secure mode, and the main processor sends periodical ON and OFF signals to the secure mode indication lamp. Then, by the keyboard manager and the decoded data transfer protocol, the disabled secure mode state may be notified on the monitor as a message type and so on, and the keyboard input information is transferred to the keyboard manager without

encryption.

In Fig.5 through Fig.7, the secure mode setup process, the secure mode clear process and key code input information processing process under the secure mode of the present invention is shown in more details.

The Fig.8 shows the data storage process after encrypting data in the secure adapter with the incorporated safe memory, and the Fig.9 shows the process to decode the encrypted data.

Those who are skilled in prior art may assume various changes and modifications within the scope of the present invention on the basis of the above description.

Brief Description of Drawings

Fig. 1 shows a configuration of the module as an embodiment of a secure adapter according to the present invention;

Fig. 2 shows a view of an embodiment of a secure adapter, of the present invention, with connection between a computer system and a keyboard using cables;

Fig. 3 shows a schematical diagram of a computer system in a computer secure system of the present invention;

Fig. 4 shows a configuration of a module that the safe memory is incorporated to a secure adapter of the Fig.1;

Fig. 5 shows steps for secure mode setup in the present invention;

Fig. 6 shows steps for clearing secure mode in the present invention;

Fig. 7 shows steps for processing key code input information under secure mode;

Fig. 8 shows steps for encrypting and storing data in a secure adapter of the Fig. 4; and

Fig. 9 shows steps for decoding stored data in a secure adapter of the Fig. 4.

Industrial Applicability

If the secure adapter and the secure computer system employing thereof of the invention are used, it is possible to prevent third person from intruding into the computer system by hacking and stealing user's secrete data, for stock exchange, Internet banking, cyber transactions and other communications over the Internet, modem communications or for network data transfer.